The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/13/2010

SUBJECT:
Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities discovered in the Adobe Acrobat and Adobe Reader applications that could allow attackers to execute arbitrary code on affected systems. Adobe Reader allows users to view Portable Document Format (PDF) files. Adobe Acrobat offers users additional features such as the ability to create PDF files. These vulnerabilities can be exploited if a user opens a specially crafted file designed to take advantage of the vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:

Adobe Reader 8.2.1 and prior
Adobe Acrobat 8.2.1 and prior
Adobe Reader 9.3.1 and prior
Adobe Acrobat 9.3.1 and prior

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Fifteen security vulnerabilities have been identified in Adobe Reader and Adobe Acrobat. These vulnerabilities can be exploited if a user opens a specially crafted file designed to take advantage of the vulnerabilities. The vulnerabilities are as follows:

- A cross-site scripting vulnerability affects an unspecified script.
- A remote code-execution vulnerability affects an unspecified prefix protocol handler.
- Three denial-of-service vulnerabilities affect unspecified vectors. Remote code-execution has not been ruled out.
- Four remote code-execution vulnerabilities caused by unspecifiedmemory corruption.
- A remote code-execution vulnerability caused by an error in font handling.
- Four unspecified buffer-overflow vulnerabilities resulting in remote code-execution.
- A heap-based buffer-overflow vulnerability could result in remote arbitrary code-execution.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Adobe to vulnerable systems immediately after appropriate testing.
- Systems running Adobe Reader 9.3.1 and Acrobat 9.3.1 and earlier versions should be updated to version 9.3.2.
- Systems running Adobe Reader 8.2.1 and Acrobat 8.2.1 and earlier versions should be updated to version 8.2.2.
- Do not open email attachments from unknown or un-trusted sources.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Adobe:
http://www.adobe.com/support/security/bulletins/apsb10-09.html

Security Focus:
http://www.securityfocus.com/bid/39329

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0190
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0191
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0192
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0193
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0194
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0195
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0196
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0197
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0198
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0199
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0201
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0202
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0203
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0204
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1241